Prevention, disruption and deterrence of online child sexual exploitation and abuse

ERA Forum
https://doi.org/10.1007/s12027-020-00625-7

ARTICLE

Prevention, disruption and deterrence of online child sexual exploitation and abuse

Ethel Quayle[1]

Abstract European law has recognised the need for international cross-disciplinary collaboration to both identify, locate and safeguard victims and prevent, investigate and prosecute online child exploitation and abuse (OCSEA). However, there is evidence that these crimes are continuing to increase and develop in step with technological advances. Changing the behaviour of both perpetrators and victims is both challenging and expensive and there is little evidence of what works to reduce these crimes. In this paper an argument is presented that changing the environments which support OCSEA is necessary if we are to detect and manage these crimes, and more importantly prevent them.

Keywords Child sexual abuse · Internet · Affordances · Prevention

1 Introduction

In a report commissioned by the Council of Europe it was noted that Online Child Sexual Exploitation and Abuse (OCSEA) does not respect national jurisdictions and that there was a need for national and international cross-disciplinary collaboration to identify, locate and safeguard victims and prevent, investigate and prosecute these crimes.[1] It was also acknowledged that any such co-operation would require the ability to respond to technological change and the corresponding changes in offender behaviour. Perhaps the most important international law instrument dedicated to the

[1] *Carr, J.* [8].

✉ E. Quayle
Ethel.Quayle@ed.ac.uk

[1] Professor of Forensic Clinical Psychology, COPINE Research, Clinical & Health Psychology, School of Health in Social Science, University of Edinburgh, Teviot Place, Edinburgh, UK

Published online: 23 September 2020

rights of the child is the UN Convention on the Rights of the Child (CRC)[2] with Article 34 of the CRC requiring states to 'protect the child from all forms of sexual exploitation and sexual abuse'. It also makes specific reference to preventing 'the exploitative use of children in pornographic performances and materials'. The Optional Protocol to the CRC on the Sale of Children, Child Prostitution, and Child Pornography (OPSC) which followed covered many forms of sexual abuse and exploitation and specifically referred to child pornography.[3] Article 2(c) of the OPSC defines child pornography as 'any representation, of whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes' which provided a wider definition that other international instruments.[4] Gillespie has argued that the region which has paid the most attention to the issue of child exploitation and in particular child sexual abuse materials (CSAM) is Europe, with both the Council of Europe and the European Union enacting international instruments that specifically relate to the issue of the sexual exploitation of a child, including through child pornography.[5]

The Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse CETS 201 (Lanzarote Convention) and the Convention on Cybercrime CETS 185 (Budapest Convention) provide comprehensive benchmarks for both criminal law and procedural law standards to prevent and combat OCSEA.[6] They build on the international standards set out by the UNRC and the OPSC designed to protect children. Articles 18 to 29 of the Lanzarote Convention and Article 9 of the Budapest Convention set out the substantive criminal law and definitions of offences required to be transposed into national law. This convention was the first instrument to establish the various forms of child sexual abuse as criminal offences including abuse committed in the home or family, with the use of force, coercion or threats. The articles specifically relevant to OCSEA offences are Articles 20 to 23 of the Lanzarote Convention, which focus specifically in Article 20 on criminalising the production, distribution and possession of, and knowing access to child pornography (increasingly referred to as CSAM[7]), offences concerning the participation of a child in pornographic performances (Article 21), the corruption of children through intentional exposure to sexual activities (Article 22) and the solicitation of children for sexual purposes (Article 23). In the European Union, Article 6.2 of the Directive 2011/92/EU of the European Parliament and Council on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography requires EU Member States to take the necessary measures to ensure that attempts to solicit a child to provide CSAM are punishable. Article 23 of the Lanzarote Convention requires states to criminalise the intentional proposal of an adult to meet a child for the purpose of unlawful sexual activity. The 2015 Opinion of the Lanzarote Committee on Article 23 of the Convention noted that "The solicitation of

[2] UN Commission on Human Rights, *Convention on the Rights of the Child*., 7 March 1990, E/CN.4/RES/1990/74.

[3] A/RES/54/263 of 25 May 2000.

[4] *Gillespie, A.A.* [25].

[5] *Gillespie* [26].

[6] *Baines, V.* [2].

[7] *Greijer, S. and Doek, J.* [28].

children through information and communication technologies does not necessarily result in a meeting in person. It may remain online and nonetheless cause serious harm to the child. The sexual offences which are intentionally perpetrated during an online meeting through communication technologies are often linked to the production, possession and transmission of child pornography" (p6).[8] Of some importance here is that the assumption of harm which underpins most legislation largely relates to the production of CSAM[9] and until recently there has been little research that has explored the 'additional harms' that come through the possession and distribution of this material.[10,11,12,13]

In a joint initiative by the EU and the United States, in 2012 54 countries from around the world signed up to a Global Alliance against Child Sexual Abuse Online. They committed to key policy targets that aim at: a larger number of rescued victims, more effective prosecution, and an overall reduction in the number of child sexual abuse images available online. The Global Alliance subsequently merged with the UK's WeProtect initiative to form the WeProtect Global Alliance to end child sexual exploitation online, which brought together over 80 governments, 20 global technology companies and 24 leading international and non-governmental organisations to protect children from sexual exploitation online. The Global Alliance (2016) produced, 'Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response' to provide guidelines and support on how to achieve the commitments. The Model was intended to enable a country to assess its current response and identify gaps, prioritise national efforts to fill gaps and enhance international understanding and cooperation. Its purpose is not prescriptive, but aims to describe the capabilities needed for effective child protection, highlight good practice from countries that are already delivering these capabilities, and signpost organisations that can provide further guidance and support to countries seeking to develop or enhance their existing capability. This tool is an interesting development as it brings together, in an accessible format, international frameworks as well as the substantial contributions made by organisations such as the United Nations, ECPAT and ICMEC.

2 Scale of the problem

In September 2019 the New York Times noted that in the previous year technology companies reported to the US National Center for Missing and Exploited Children (NCMEC) over 45 million photographs and videos of children being sexually abused. This was more than twice the number reported in the previous year.[14] The

[8] Lanzarote Committee - Opinion on Article 23 of the Lanzarote Convention and its explanatory note (2016). Available at: https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html.

[9] *Hessick, C.B.* [29].

[10] *Gewirtz-Meydan, A., et al.* [23].

[11] *Gassó, A., et al.* [22].

[12] *Maas, M., et al.* [40].

[13] *Pashang, S., et al.* [54].

[14] *Keller, M.H. & Dance, G.J.X.* [36].

article made reference to research completed in 2019 in collaboration with NCMEC which stated that "... online sharing platforms have accelerated the pace of CSAI [child sexual abuse image] content creation and distribution to a breaking point where NCMEC's manual review capabilities and law enforcement investigations no longer scale" (p1).[15] This study used anonymised metadata associated with the 23,494,983 NCMEC reports related to suspected CSAI that were received from March, 1998 (when NCMEC's CyberTipline was created) until September 2017. NCMEC reports come from the US public and many US ESPs (electronic service providers) and over 9.6 million such reports (40%) occurred in the year 2017 (approximately one million per month) compared to the 565 000 reports (2.4%) in its first ten years of operation.

While meaningful estimates of these crimes are highly problematic,[16] it has been argued that there are essentially four ways in which online-facilitated child sexual abuse (OCSA) can be measured: by counting the number of offences committed, the number of perpetrators, the number of victims and the number of images that have been viewed, downloaded and exchanged. However, these authors note that quantification based on each of these four measures inevitably produces very different figures, partly because they are attempting to count different aspects of OCSA. However, there is converging evidence that sexual image-related crimes against children are increasing, although a recent meta-analysis of the prevalence of online solicitation amongst youth (one specific form of online child sexual abuse) would indicate that one in nine young people experience online solicitation, although prevalence rates have decreased over time.[17]

3 Cybercrime

Online child sexual abuse (OCSA) can be positioned as a cybercrime in which technology plays a role across a broad spectrum of activities. The definition of cybercrime has been described as highly contentious, as while many people agree that cybercrime exists, they are not really clear what it is.[18] In this respect, cybercrime has developed from earlier concepts of computer crime and e-crime and has broadened to cover many different forms of criminal activity. The European Crime Prevention Network[19] has also argued that there is a current absence of any consistent definition, and even within specific legislative documents cybercrime is used in different ways. For example, the Council of Europe Cybercrime Convention uses broad criminalisation headings in its definition of cybercrime, including 'offences against the confidentiality, integrity and availability of computer data and systems,' 'computer-related offences', 'content-related offences' and 'copyright-related offences'.[20]

[15] *Bursztein, E., et al.* [7].

[16] *Wager, N., et al.* [71].

[17] *Madigan, S., et al.* [41].

[18] *Wall, D.S.* [72].

[19] EUCPN. Cybercrime: a theoretical overview of the growing digital threat. In: EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network: Brussels (2015).

[20] Council of the European Union. Convention on Cybercrime, Budapest, 23 November (2001).

Many researchers and practitioners[21] use 'cyber-dependent crime' and 'cyber-enabled crime' or 'cyber-assisted crime' to classify different forms of cybercrime. At one end of the cybercrime spectrum there is 'cyber-assisted' crime in which the Internet is used in its organisation and implementation, but which would still take place if the Internet was removed (e.g. a potential offender using online social media to locate a child who is sexually assaulted off-line). At the other end of the spectrum is 'cyber-dependent' crime, which exists because of the Internet, such as DDoS (distributed denial-of-service) attacks or spamming. Differentiating between cyber-assisted crime and cyber-enabled crime is at times very difficult, but it would appear that the boundaries between cybercrime and traditional forms of crime have never been clear cut and are becoming increasingly blurred due to the level of hyper-connectivity in today's highly digitised and networked world.[22] The ubiquitous use of the Internet and smart mobile devices in people's everyday lives, the wide adoption of cloud-based services by industry and government, and, for example, the advent of the Internet of Things (IoT), the Internet of Everything (IoE), and Cyber-Physical Systems (CPSs), have led to the widely accepted belief that almost all criminal activities include some cyber elements.[23] As a consequence, digital forensics (sometimes called cyber forensics) have become an essential part of almost all crime investigation processes for law enforcement around the world.[24]

The United Nations Office on Drugs and Crime[25] also argues that there is no international definition of cybercrime or cyberattacks, but while they use the cyber-enabled-cyber-dependent dichotomy, they add a further specific-crime type: online child sexual exploitation and abuse, which includes abuse on the clear internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion - known as "sextortion". Quayle expanded these crimes to include the production, dissemination and possession of child sexual abuse images (known in many jurisdictions as child pornography); online grooming of children for sexual purposes; 'sexting'; sexual extortion of children ('sextortion'); revenge pornography; commercial sexual exploitation of children; exploitation of children through online prostitution, and live streaming of sexual abuse.[26] Other authors have defined OCSA as sexual abuse of children involving force or enticement to take part in sexual activities where the online environment is involved at any stage of the offence.[27] This includes the production, preparation, consumption, sharing, dissemination or possession of child sexual abuse material and the solicitation of children for sexual purposes of children (sometimes called 'grooming'), whether or not it results, or is intended to result, in a contact offence. In high to middle income countries, technology now mediates almost all human activities in some ways, including those of children, which makes

[21] *McGuire, M. & Dowling, S.* [45].

[22] *Sarre, R., et al.* [60].

[23] *Miraz, M., et al.* [49].

[24] EUROPOL. Internet organised crime threat assessment (2018). Available at: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

[25] UNOCDC Cybercrime (2019). Available at: https://www.unodc.org/unodc/en/cybercrime/index.html.

[26] *Quayle, E.* [55].

[27] *May-Chahal, C., Palmer, E.* [44].

an analysis of clear distinctions between offline and online abuse difficult. Digital technologies are embedded in our everyday practices and form an intrinsic part of private and public experiences. Yet whilst creating opportunities for children to act as receivers, participants and actors in the digital world, the Internet also creates spaces of social interaction which hold the potential for exposure to online risks, including sexual risks such as abuse and exploitation.

4 Cybercrime migration?

What is important to note, is that while there is converging evidence in some countries to support falling rates of non-technology-mediated child victimisation, including child sexual abuse[28,29,30,31] this does not appear to be the case in relation to some forms of OCSA. It is easy to speculate as to whether there is a relationship between the decrease in offline CSA and an increase in OCSA, and whether there has been a migration from one to the other. It is, however, much more difficult to evidence this. Probably the largest number of convictions for cyber sexual crimes relate to possession of CSAM[32] and this may relate to the forensic evidence available for law enforcement to secure a conviction.[33] Many, if not all, people charged with possession will have a 'permanent product' of that crime available to law enforcement: pictures and videos depicting child abuse and exploitation that meet the criteria in that jurisdiction for illegality. It might be argued that this (as opposed to the evidence required for prosecution of a contact offence against a child) will increase the number of successful convictions. However, though not without its critics, the 'cybercrime hypothesis' has been used to account for a reduction of crime in other areas.[34]

Miró-Llinares and Moneva present two hypotheses which they argue highlight the essential role of cyberspace as an environment that has shifted criminal opportunities from physical to virtual space and which ultimately reflects on crime trends.[35] The first hypothesis provides evidence that the more time spent at home by many young people engaging with, for example, video games and other online activities, could have had an impact on the drop in juvenile crime. Their second hypothesis states, which has relevance for this paper, that the appearance of cyberspace has led to a shift in opportunities from physical space to cyberspace. This seems particularly pertinent in relation to online grooming or sexual solicitation. For example, a survey of law enforcement[36] indicated that social networking sites (SNSs) were used to initiate

[28] *Finkelhor, D., Jones, L.* [19].

[29] *Laaksonen, T., et al.* [37].

[30] *Dunne, M., et al.* [15].

[31] *Shields, M., et al.* [63].

[32] *Wolak, J., et al.* [75].

[33] *Walsh, W., et al.* [73].

[34] *Farrell, G., Birks, D.* [17].

[35] *Miro-Llinares, F., Moneva, A.* [50].

[36] *Mitchell, K.J., et al.* [51].

sexual relationships, to provide a means of communication between victim and offender, to access information about the victim, to disseminate information or pictures about the victim, and to get in touch with the victim's friends; SNSs might be said to 'afford' opportunities for offending. In a similar way, what has been noted in offender samples is the ease that online sexual behaviour can take place, often prompted by the easy exchange of photographs, text or the presence of web cameras, without any physical contact, or the risks that would be associated with it.[37]

5 Affordances

Positioning OCSEA as cybercrimes forces us to think about the context in which these abuses and exploitations take place. This potentially may offer ways of preventing or managing these crimes and moves us away from a focus on the characteristics of offenders or their victims (and how it may be possible to effect changes in *their* behaviour). In the context of young people's mental health and digital environments it has been suggested that digital technologies have their own affordances, which are listed as persistence, replicability, scalability and searchability.[38] The affordances of digital technology (in conjunction with the capabilities of online and networked technology such as social media) allow digital information to be easily copied (replicability), easily shared with large audiences (scalability), easily recorded and archived (persistence), and easily accessed by others and found in the future (searchability). Livingstone argues that these affordances are:

> "the result of complex networked infrastructures invented and implemented by people working under huge pressure and at speed in, largely, commercial institutions with global ambitions. That means the needs of vulnerable young people may come very low down in their list of priorities. How far researchers, clinicians and other practitioners can wrest back control to ensure digital networks meet the best interests of young people is as yet unknown, though surely a struggle worth the effort".[39]

This has been explored in the context of 'revenge porn' (non-consensual intimate image distribution) where it is argued that replicability and scalability have increased the ease with which such an act can be committed and the ease with which a nude/sexual image can be distributed to a large audience.[40] Persistence and searchability have also augmented impact of this act in some cases by allowing this content to be located by others and to potentially affect a victim at some point in the future. However, Dodge is critical of the decontextualised ways in which, for example the judiciary have universally used these digital affordances to justify harsh sentences and this is further explored in a discussion of 'affordances-in-practice' which stresses the

[37] *Quayle, E., et al.* [57].

[38] *Boyd, D.* [3].

[39] *Livingstone, S.* [38].

[40] *Dodge, A.* [14].

idea that 'affordances are not intrinsic properties that can be defined outside their situated context of usage, but ongoing enactments by specific users that may vary across space and time' (p3653).[41]

The term 'affordance' is used throughout this paper and this warrants further discussion. For Gibson, affordances referred to the possibilities that an object offers for action, where the properties of the object emerge through the interaction between actors and those objects.[42] This is not only related to the physical properties of the object but also to social norms and rules.[43] The concept was further developed in relation to human-computer interaction, where it was argued that an affordance should not be understood as a property but rather as a relationship.[44] It is therefore not a static feature of an object and whether an affordance exists depends entirely on the relationship between the actor and the property. Norman argued that the concept of affordances does not imply that online practices are determined by technology, but rather by how people use it. Therefore, affordances are not static features of technology, but have a number of potential actions associated with them. An affordance exists once a user has perceived it and perceived the potential actions associated with it. For example, Voice over Internet Protocols (such as Skype) have not only been used by many people to keep in touch with geographically distant family members[45] but also to facilitate the live streaming of sexual abuse of children. There are reports of live streaming in South Asia with victims described as deprived children who are coerced into live streaming of sexual abuse, from computers provided by employers, against their will.[46] However, live streaming has also been reported in high-income countries such as the UK.[47] Live streaming provides real-time access to events for participants who are not actually engaging in the activity themselves. The UK's National Crime Agency's strategic assessment of serious organised crime suggested that "the practice of live streaming is one example of how offenders can simultaneously create indecent images of children (IIOC) online, view IIOC, and commit contact abuse by proxy overseas".[48] A case study on Periscope (a live streaming platform) provides a forensic examination of the technical and legal challenges for the investigation of live streaming of sexual abuse.[49] This is a good illustration of how actors may use technologies in creative and unpredictable ways.[50]

[41] *Costa, E.* [12].

[42] *Gibson, J.J.* [24].

[43] *Meredith, J.* [46].

[44] *Norman, D.A.* [53].

[45] *Share, M., et al.* [62].

[46] *Brown, R., et al.* [6].

[47] Internet Watch Foundation (2018). Available at: https://www.iwf.org.uk/news/iwf-research-on-child-sex-abuse-live-streaming-reveals-98-of-victims-are-13-or-under.

[48] National Crime Agency. National strategic assessment of serious and organised crime 2016. Available at: http://www.nationalcrimeagency.gov.uk/publications/731-national-strategic-assessment-of-serious-and-organised-crime-2016/file.

[49] *Horsman, G.* [30].

[50] *Jarzabkowski, P., Kaplan, S.* [31].

It has also been argued that the Internet creates affordances that facilitate innovative ways of committing old and new crimes[51] and Jerde suggests child sexual abuse material (CSAM) as an example of crime that uses Internet affordances to "circumvent law enforcement techniques deployed around national borders to avoid detection"[52] (p 2). A further study in the context of cyberbullying on social networking sites (SNSs) used affordance to refer to the mutuality of actor intentions and technology capabilities that provide the potential for a particular action.[53] This relational view of affordance is seen as advantageous for understanding technology use because it allows us to consider the symbiotic relationship between the capabilities of the technology and the actor's goal and actions. It has been argued that the actualisation of affordances occurs when an actor takes advantage of one or more affordances of SNSs to achieve immediate concrete outcomes that support their goals. The focus is therefore on contextualised actions that technology makes qualitatively easier[54] but which may be specific to that relationality and which potentially move researchers away from the certainties of separate technology attributes and actors' attitudes.[55]

6 Technological affordances and CSAM

Technological affordances have also been considered in the context of an interaction between design and usage and an example of this is privacy settings, where affordances shape practice in that privacy settings distinguish between public, private or partially private communications.[56] However, as previously noted, users also shape affordances, for example, young people setting up multiple profiles on SNSs to project different selves to different audiences. Earlier work in this area suggested that we can also identify 'social affordances' that refer to interactions between how users respond, the social context and social networks.[57] However, it has been argued that other people provide the richest and most significant environmental affordances.[58] One finding, of interest in relation to online grooming of children, is that technological affordances are related to the motivations people have for using them. It is not only important to think about what these 'action possibilities' are, but when and for whom they might happen. For adolescents this may relate to the developmental task of exploring sexuality, afforded through the ability to create sexual media, the online applications that support this (e.g. WhatsApp, Instagram), and the peer and adult engagement with this digital content. Of importance, it has been noted that new technologies reshape public life, but teens' engagement also reconfigures the technology itself. In the context of technology-mediated CSA, consideration of the reciprocity of

[51] *Robey, D., et al.* [59].

[52] *Jerde, R.* [32].

[53] *Chan, T., et al.* [9].

[54] *Earl, J., Kimport, K.* [16].

[55] *Majchrzak, A., et al.* [42].

[56] *Staksrud, E., et al.* [64].

[57] *Wellman, B., et al.* [74].

[58] *Kaufmann, L., Clément, F.* [35].

this engagement needs to be widened to include another set of actors - those motivated by a sexual interest in children.

Crime opportunity theory[59] and the affordance perspective has been used to develop a meta-framework to inform an understanding of SNS bullying.[60] Specifically, crime opportunity theory argues that two primary components contribute to a crime being committed: a likely perpetrator, and environmental conditions that offer criminogenic opportunities. In this context using an affordance perspective into crime opportunity theory helped explain how social media allows a perpetrator to evaluate whether environmental conditions would facilitate SNS bullying activity. In their empirical study they proposed two SNS environmental conditions that offered criminogenic opportunities for a likely offender to engage in SNS bullying. These were the presence of suitable targets and the absence of capable guardianships. The affordances that facilitated the identification of suitable targets, and which have relevance for technology-mediated sexual abuse offences, were accessibility, information retrieval, editability, and association. The first two of these (accessibility and information retrieval) are particularly salient for OCSA crimes. Accessibility affordance allows a perpetrator to transcend time and spatial constraints to reach potential targets and provides the opportunity to connect with an unlimited number of users, including people who are known and also unknown, leading to an environment where suitable targets can be identified and accessed. Information retrieval affordance refers to the extent to which a user believes that an SNS offers the opportunity to obtain information about a user on that platform. This allows a likely offender to access material created by a potential target, which provides information about the background, preferences, and daily activities of that individual. These authors note that SNS updates often include new features that encourage users to continuously create and share information on these platforms.

Earlier work had also used these frameworks to understand CSAM-related crimes.[61] Their starting point was routine activity theory [62] which identified three minimal elements for criminal action: i. a likely offender; ii. a suitable target, and iii. absence of a capable guardian. Focus on access to a suitable target, as with the meta-framework developed in relation to bullying, drew attention to the context in which potential criminal activity takes place which can be modified or changed. This moves the focus away from the 'likely offender' and the likely circumstances (both distal and proximal) that might have influenced their behaviour to the possibility of changing the environment in a way that increases or supplements the availability of capable guardianship. It distinguishes between the inclination to offend and the actual offence. Analysing criminal activity, which is both particular and grounded in its situational context, should therefore relate to the context and circumstances of a particular situation.

In the context of CSAM, the absence of a capable guardian seems particularly pertinent. In November 2019 the BBC news reported (along with other agencies) the

[59] *Felson, M., Clarke, R.* [18].

[60] Ibid. 29.

[61] *Taylor, M., Quayle, E.* [68].

[62] *Cohen, L.E., Felson, M.* [10].

decision by Facebook to encrypt all of its messenger services, 'The end-to-end encryption on Facebook-owned WhatsApp will be extended to Facebook Messenger and Instagram, with Mr Zuckerberg [CEO Facebook] acknowledging there would be a "trade-off" that would benefit child sex abusers and other criminals'.[63] While there is limited evidence for the purposeful use of encryption by offenders to conceal online sexual activities against minors,[64] tools such as WhatsApp, which have end to end encryption, protect the data during transmission (and storage) by default.[65] This also means that the applications used by organisations such as NCMEC and the Internet Watch Foundation (IWF) to detect and remove CSAM content (such as PhotoDNA) may no longer have the same efficacy. PhotoDNA creates a unique digital signature ("hash") of an image which is then compared with hashes of other photos to find copies of the same image. When matched with a database containing hashes of previously identified illegal images, PhotoDNA helps detect, disrupt and report the distribution of child exploitation material.[66] Paradoxically, encryption by default may provide an environment which perpetuates the sense of privacy and anonymity associated with such applications. A recent study, albeit within a different context, concluded that new app developers need to be mindful of the affordances of the products they develop,[67] and in terms of online child protection this may be crucial.

7 Criminogenic qualities of the Internet

Recently there have been a number of studies examining the criminogenic qualities of the Internet.[68,69] It has been argued that situations vary in their criminogenic qualities (producing or leading to crime), from those that challenge offenders by requiring them to create opportunities, through those that provide easy temptations, to those that actively provoke crime.[70] Importantly, Wortley considers the interaction between criminogenic environments and the criminogenic disposition of the likely offender. The latter has its roots in an offender typology which is based on the strength of criminal dispositions and the different roles played in their crimes by the immediate environment.[71] In this typology, anti-social predators may actively seek out criminal opportunities and use situational information to make rational choices about the risks and benefits of committing an act. Mundane offenders engage in low-level crime and seem to demonstrate poor self-control and succumb easily to the opportunities offered in a given situation. The final category, provoked offenders, are less

[63] BBC News. Facebook removes 11.6 million child abuse posts (2019). Available at: https://www.bbc.co.uk/news/technology-50404812.

[64] *Steel, C., et al.* [66].

[65] *Loeb, J.* [39].

[66] Microsoft PhotoDNA (2019). Available at: https://www.microsoft.com/en-us/PhotoDNA.

[67] *Moreno, M.A., D'Angelo, J.* [52].

[68] *Reyns, B., et al.* [58].

[69] *Brewer, R., et al.* [5].

[70] *Wortley, R.* [76].

[71] *Cornish, D.B., Clarke, R.V.* [11].

likely to have a criminal record but react to an array of situational conditions, some which may be internal and others environmental. Related to this, Seto described a motivation-facilitation model of sex offending which examined the relationships between paraphilic traits (predispositions), state factors (which facilitate acting on these predispositions) and situational factors (access and presence of a capable guardian).[72] This was examined in the context of CSAM offenders and concluded that many of these individuals are motivated to engage in sexual behaviour with children as they have paedophilic or hebephilic sexual interests, but that they demonstrate high levels of self-control (or low in facilitation factors). This leaves them less likely to commit a contact offence but this, in the context of access to Internet technologies, is not sufficient to inhibit acting on the opportunity to commit CSAM offences. These offenders have also been found to have greater access to technology but less access to children than contact offenders.[73]

These issues are also examined in Brewer et al.'s study on adolescent delinquency and the criminogenic features of digital technology.[74] These authors argue that the Internet exhibits features that make it uniquely criminogenic to offline environments. The Internet as a distinct 'place' is said to de-territorialize encounters which are no longer limited by geography and can take place in synchronous or asynchronous time, which enable identity and motives to remain concealed. They suggest that, 'Users can easily move from a point of predictable use (e.g. targeted information searches) to apparently random and unpredictable discoveries of information, images and points of view due to the multiple 'hidden' linkages between websites and services that are often driven by commercial considerations" (p 118). Algorithms may also direct or nudge users to certain content or services based on past individual or collective activity. It has been argued that these algorithms can be specifically designed to capitalize on cravings and curiosities (and they may well have affordance qualities).[75]

A topical example of this relates to YouTube's video recommendation system which displays on a sidebar what is 'up next' for the viewer.[76] These are ranked according to the user's history and context, and newer videos are generally preferenced. A publication in the New York Times reported that YouTube's algorithm was encouraging people with a sexual interest in children to watch videos of partially clothed minors, often after viewing videos with sexual content. These videos were often domestic and showed children at the swimming pool or on vacation, but their report claimed that there was evidence that for some of the people watching them they were serving a different (and possibly sexual) purpose.[77] A technical paper by three Google employees discussed the deep neural networks for YouTube recommendations and stated that a two-stage approach allows recommendations to be made from a very large corpus (millions) of videos while still being certain that the small num-

[72] *Seto, M.C.* [61].

[73] *Babchishin, K.M., et al.* [1].

[74] Ibid. 55.

[75] *Vaidhyanathan, S.* [70].

[76] *Matamoros-Fernández, A., Gray, J.* [43].

[77] *Fisher, M., Taub, A.* [21].

ber of videos appearing on the device are personalized and engaging for the user.[78] Our viewing history will determine what we are 'nudged' to view, and potentially for a number of individuals will increase the likelihood of viewing content that may approximate sexually inappropriate or illegal content.

It has been suggested that there are qualities of the Internet either in association with facilitating conditions (personal or environmental) or otherwise that in themselves made accessing and possession of CSAM more likely and in essence operate as 'event' factors (that relate to the commission of this particular crime).[79] This argument was framed within an analysis drawing on a situational crime control model, which emphasises the significance of pre-criminal situations and opportunity. Taylor drew parallels between terrorist activities and CSAM-related crimes and argues that some forms of user interaction with the Internet suggest the Internet may have criminogenic qualities.[80] Firstly, the distributed nature of the Internet and the corresponding lack of control over content is a factor in increased availability of illegal or undesirable material. Secondly, the way that distributed complex global microstructures develop effectively increases opportunity for access to that content. Alongside this, criminal conspiracies can deliberately and intentionally use both content and opportunity to engage with, and draw in, otherwise uncommitted people.

8 Practice implications for prevention

Changing individuals (likely offenders and likely targets) is both challenging and expensive. Over the last 20 years there has been a development of a number of internet safety and education programmes to increase positive adolescent behaviour and safety online but their findings from a systematic review of related studies suggested that there is still a need for re-evaluating how internet safety education is delivered in the future.[81] In a further publication a content analysis of four Internet Safety Education Programmes for children indicated that most were not incorporating proven education strategies and lacked any strong evidence base[82] although a more recent study does advocate for the alignment of such programmes with a clearer evidence base.[83] They also challenged whether messages would be better delivered through broader youth safety prevention programs versus stand-alone lessons. Intervention programmes that target online offenders have shown equivocal evidence. For example, the UK-accredited treatment programme (iSOTP) was assessed following completion of pre and post-psychometric assessments by 264 convicted offenders and indicated improvements in socio-affective functioning and a decrease in pro-offending attitudes.[84] An evaluation of the psycho-educational programme Inform and Inform

[78] *Covington, P., et al.* [13].

[79] *Taylor, M., Quayle, E.* [69].

[80] *Taylor, Max.* [67].

[81] *Jones, L.M., et al.* [34].

[82] *Jones, L.M., et al.* [33].

[83] *Finkelhor, D., et al.* [20].

[84] *Middleton, D., et al.* [48].

Plus, developed in the UK by The Lucy Faithful Foundation suggested that data from eleven groups indicated that participants felt enabled to face up to being arrested and/or convicted, helped them develop a greater understanding of their offending behaviour and how to establish a non-offending life.[85] However, an Impact evaluation of the UK prison-based Core Sex Offender Treatment Programme between 2000 and 2012 indicated that more treated sex offenders committed at least one child image reoffence during the follow-up period when compared with the matched comparison offenders who had received no treatment (4.4% compared with 2.9 %).[86]

It seems likely that changing the contexts in which sexual crimes take place may offer greater opportunity to effect change. Wortley (2012) comments that the most common model of situation prevention is opportunity reduction, which involves manipulating the immediate environmental contingencies so as to increase the perceived costs of offending.[87] He applies this to the problem of CSAM through an examination of three opportunity-reduction strategies: reducing perceived rewards, increasing the perceived effort and increasing the perceived risks. Reducing the rewards of CSAM may involve removing or denying access to content that is targeted by offenders through, for example, regulatory control of content by Internet Service Providers. Disruption tactics, such as blocking efforts by Google and Microsoft, resulted in a 67% drop over 12 months in web-based searches for abuse images compared with no blocking activities from Yandex.[88] There are some positive indicators in relation to Internet monitoring, moderation, and reporting of problematic content or behaviour.[89] One example is the development of a web crawler (Arachnid) by the Canadian Centre for Child Protection to detect images and videos based on confirmed digital fingerprints of illegal content and combat the proliferation of child sexual abuse material on the Internet. They report that the automated crawler helps reduce the online availability of child sexual abuse material through its identification and issuing of a notice to the hosting provider requesting its removal. As of November 2019, over 13.3 million images were identified for analyst review and 4.7 million notices were sent to providers. Of these, 85% of related to victims who are not known to have been identified by police.[90] Such disruption tactics reduce the number of images available through simple searching, which is important as the presence of easily available CSAM, and high levels of Internet use, are risk factors in Internet offending. Increasing the perceived effort of accessing CSAM involves making it more difficult for offenders to gain access to content, which means they have to expend more effort. A publication by the Mobile Alliance Against Child Sexual Abuse Content presents a collation of approaches that have been proved successful in deterring or detecting illegal or illicit use of mobile payment services used to access CSAM.[91] It is also

[85] *Gillespie, S., et al.* [27].

[86] *Mews, A., et al.* [47].

[87] Ibid. 56.

[88] *Steel, C.* [65].

[89] *Quayle, E., Koukopoulos, N.* [56].

[90] Project Arachnid. Available at: https://www.cybertip.ca/app/en/projects-arachnid.

[91] Mobile Alliance Against Child Sexual Abuse Content. Preventing mobile payment services from being misused to monetise child sexual abuse content (2014). Available at: https://www.gsma.com/

likely that increasing perceived risks may be achieved through proactive policing. One example of this is provided by the EUROPOL initiative Police2Peer which involves law enforcement informing people trying to access or share CSAM on P2P networks of the risks that they are taking and offering information as to where they can get help.

In a similar vein, attention has been drawn to the particular context in which access to CSAM occurs, which firmly locates the behaviour within the factors that influence it. These have been summarized as: the significance of high affordance cues giving access to images; immediate and highly salient reinforcement on achieving access to images; perceived absence of capable guardianship and surveillance (in a general sense as far as the Internet is concerned, and in a specific sense in terms of the privacy associated with Internet use); insensitivity to immediate negative qualities resulting from both motivational factors and the strong affordance qualities of screen based cues.[92] Three kinds of crime prevention initiatives have been identified which may be of value in helping to place this into context: primary prevention (focused on stopping a crime before it occurs); secondary prevention (directed at people thought to be at high risk of committing an offence) and tertiary prevention (focused on known offenders).[93] These categories were used to explore prevention efforts in relation to CSAM using two additional crime prevention categories: reducing provocation and removing excuses. Removing excuses (for example, through informing target audiences of the illegality of CSAM and its associated harms to children) through media campaigns have provided evidence that these represent an effective way to reach a large audience and transmit the messages that there are significant consequences to viewing CSAM, individuals have personal responsibility in controlling their behaviour, and that help is available. In this respect, campaigns appear to be an appropriate strategy for deterring people from viewing CSAM, that sits alongside other initiatives.[94]

9 Conclusion

While there is no evidence to suggest that online abuse and exploitation are more serious or pervasive offences than crimes occurring offline, it is the case that the affordances offered by online social media may present a significant risk factor for some children. Three factors play an important role in this complex and dynamic scenario: potential perpetrators and victims, the social context in which criminal activities take place and the rapidly changing medium. In this paper an argument has been presented that changing the environments that supports OCSA is necessary if we are to detect and manage these crimes, and more importantly prevent them. In

publicpolicy/wp-content/uploads/2016/09/GSMA2014_Report_PreventingMobilePaymentServicesFromBeingMisusedToMonetiseChildSexualAbuseContent.pdf.

[92] Ibid. 75.

[93] *Brantingham, P., & Faust, F.A.* [4].

[94] Newman, E., Efthymiadou, E., Stelzmann, D., Quayle, E., Squire, T., Beier, K., von Heyden, M., Wagner, J., Koukopoulos, N., Wortley, R. Campaigns to Deter Viewing of Child Sexual Abuse Images Online: Results of Two Campaign Cases in Europe (2019). London, NSPCC.

2019 the Child Dignity Alliance produced a Technical Working Group Report which examined the role of technology in combating the proliferation of online child sexual exploitation and abuse imagery. Critically, the report recommended that IT companies such as Facebook, Google and Microsoft should continue to: support the efforts of law-enforcement, government and non-profit agencies through sharing key technical and operational data; to share technology that tackles child sexual abuse imagery; to share operational data about those abusing their networks; to improve the verification of customer identity when new domains are registered or renewed, and to proactively identify threat actors and vulnerable users. Such changes, along with the technical solutions that flow from them, offer the only scalable interventions in relation to these crimes. Yet it is clear that prevention of OCSA is in its infancy and that, as argued by Carr, the response from the IT industry in increased proactive deployment and effectiveness of tools used to detect and deter CSAI is, while welcome, still partial with many of the key organisations not fully engaged.[95]

References

1. Babchishin, K.M., Hanson, R.K., VanZuylen, H.: Online child pornography offenders are different: a meta-analysis of the characteristics of online and offline sex offenders against children. Arch. Sex. Behav. **44**, 45–66 (2015). https://doi.org/10.1007/s10508-014-0270-x
2. Baines, V.: Member state responses to prevent and combat online child sexual exploitation and abuse (2019). Available at https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109
3. Boyd, D.: Taken out of context: American teen sociality in networked publics. ProQuest Dissertations and Theses (2008)
4. Brantingham, P., Faust, F.A.: Conceptual model of crime prevention. Crime Delinq. **22**(3), 284–296 (1976)
5. Brewer, R., Cale, j., Goldsmith, A., Holt, T.: Young people, the Internet, and emerging pathways into criminality: a study of Australian adolescents. Int. J. Cyber Criminol. **12**(1), 115–132 (2018)
6. Brown, R., Napier, S., Smith, R.: Australians who view live streaming of child sexual abuse: an analysis of financial transactions. Trends & Issues in Crime and Criminal Justice **589** (2020)
7. Bursztein, E., Bright, T., DeLaune, M., Elifff, D.M., Hsu, N., Olson, et al.: Re-thinking the detection of child sexual abuse imagery on the Internet. In: Proceedings of the 2019 World Wide Web Conference, WWW '19, May 13–17, 2019, San Francisco, CA, USA (2019)
8. Carr, J.: Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse. Council of Europe (2019). Available at https://childhub.org/en/system/tdf/library/attachments/191120.comparative_reviews_-_web_version_1.pdf.pdf?file=1&type=node&id=40893
9. Chan, T., Cheung, C., Wong, R.: Cyberbullying on social networking sites: the crime opportunity and affordance perspectives. J. Manag. Inf. Syst. **36**(2), 574–609 (2019)

[95] *Carr, J.* [8].

10. Cohen, L.E., Felson, M.: Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. **44**(4), 588–608 (1979)
11. Cornish, D.B., Clarke, R.V.: Opportunities, precipitators and criminal dispositions: a reply to Wortley's critique of situational crime prevention. In: Smith, M.J., Cornish, D.B. (eds.) Theory for Practice in Situational Crime Prevention. Crime Prevention Studies, vol. 16. Criminal Justice Press, Monsey (2003)
12. Costa, E.: Affordances-in-practice: an ethnographic critique of social media logic and context collapse. New Media Soc. **20**(10), 3641–3656 (2018)
13. Covington, P., Adams, J., Sargin, E.: Deep neural networks for YouTube: recommendations. In: Proceedings of the 10th ACM Conference on Recommender Systems, Boston, Massachusetts, USA (2016). 978-1-4503-4035-9
14. Dodge, A.: Nudes are forever: judicial interpretations of digital technology's impact on "revenge porn". Can. J. Law Soc. **34**(1), 121–143 (2019)
15. Dunne, M., Purdie, D., Cook, M., Boyle, F., Najman, J.: Is child sexual abuse declining? Evidence from a population-based survey of men and women in Australia. Child Abuse Neglect **27**(2), 141–152 (2003)
16. Earl, J., Kimport, K.: Digitally Enabled Social Change. MIT Press, Cambridge (2011)
17. Farrell, G., Birks, D.: Did cybercrime cause the crime drop? Crime Sci. **7**(8), 1–4 (2018). https://doi.org/10.1186/s40163-018-0082-8
18. Felson, M., Clarke, R.: Opportunity Makes the Thief: Practical Theory for Crime Prevention. The Policing and Reducing Crime Unit, London (1998)
19. Finkelhor, D., Jones, L.: Why have child maltreatment and child victimization declined? J. Soc. Issues **62**(4), 685–716 (2006)
20. Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., Collier, A.: youth Internet safety education: aligning programs with the evidence base [published online ahead of print]. Trauma Violence Abuse, (2020). 2020;1524838020916257. https://doi.org/10.1177/1524838020916257
21. Fisher, M., Taub, A.: On YouTube's digital playground, an open gate for pedophiles (2019). Available from https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html?module=inline
22. Gassó, A., Klettke, B., Agustina, J., Montiel, I.: Sexting, mental health, and victimization among adolescents: a literature review. Int. J. Environ. Res. Public Health **16**(13), 2364 (2019)
23. Gewirtz-Meydan, A., Lahav, Y., Walsh, W., Finkelhor, D.: Psychopathology among adult survivors of child pornography. Child Abuse Neglect **98**, 104189 (2019)
24. Gibson, J.J.: The Ecological Approach to Perception. Houghton Mifflin, London (1979)
25. Gillespie, A.A.: Defining child pornography: challenges for the law. Child Fam. Law Q. **22**, 200–222 (2010)
26. Gillespie: Child pornography. Inf. Commun. Technol. Law **27**(1), 30–54 (2018). https://doi.org/10.1080/13600834.2017.1393932
27. Gillespie, S., Dervley, R., Squire, T.: Internet offenders and "Inform Plus": an evaluation of a community based groupwork programme. NOTA News **75**, 19–20 (2015)
28. Greijer, S., Doek, J.: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016). Available at https://www.unicef.org/protection/files/Terminology_guidelines_396922-E.pdf
29. Hessick, C.B.: Disentangling child pornography from child sex abuse. Wash. Univ. Law Rev. **88**(4), 853 (2011)
30. Horsman, G.: A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: a case study on Periscope. J. Inf. Secur. Appl. **42**, 107–117 (2018)
31. Jarzabkowski, P., Kaplan, S.: Strategy tools-in-use: a framework for understanding "technologies of rationality" in practice. Strateg. Manag. J. **36**(4), 537–558 (2015)
32. Jerde, R.: Follow the Silk Road: How Internet affordances influence and transform crime and law enforcement. Master's Dissertation from the Naval Postgraduate School Monterey, CA (2017)
33. Jones, L.M., Mitchell, K., Walsh, W.A.: A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used? Crimes Against Children Research Center (CCRC), University of New Hampshire, Durham (2014)
34. Jones, L.M., Mitchell, K.J., Walsh, W.A.: A Systematic Review of Effective Youth Prevention Education: Implications for Internet Safety Education. Crimes Against Children Research Center (CCRC), University of New Hampshire, Durham (2014)
35. Kaufmann, L., Clément, F.: How culture comes to mind: from social affordances to cultural analogies. Intellectica **46**, 1–36 (2007)

36. Keller, M.H., Dance, G.J.X.: The Internet is overrun with images of child sexual abuse. What went wrong? (2019). Available at https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html
37. Laaksonen, T., Sariola, H., Johansson, A., Jern, P., Varjonen, M., Von Der Pahlen, B., et al.: Changes in the prevalence of child sexual abuse, its risk factors, and their associations as a function of age cohort in a Finnish population sample. Child Abuse Neglect **35**(7), 480–490 (2011)
38. Livingstone, S.: What are the key issues for research and intervention in the field of youth mental health? And how might the digital environment play into this? (2019). Available at https://blogs.lse.ac.uk/parenting4digitalfuture/2019/11/06/what-are-the-key-issues-for-research-and-intervention-in-the-field-of-youth-mental-health-and-how-might-the-digital-environment-play-into-this/
39. Loeb, J.: Europol study assesses technology for fighting online child abuse. Engineering Technology **12** (2017)
40. Maas, M., Bray, K., Noll, B.: Online sexual experiences predict subsequent sexual health and victimization outcomes among female adolescents: a latent class analysis. J. Youth Adolesc. **48**(5), 837–849 (2019)
41. Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J.R., Browne, D., Dimitropoulos, G.: The prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis. J. Adolesc. Health **63**(2), 133–141 (2018)
42. Majchrzak, A., Faraj, S., Kane, G., Azad, B.: The contradictory influence of social media affordances on online communal knowledge sharing. J. Comput.-Mediat. Commun. **19**(1), 38–55 (2013)
43. Matamoros-Fernández, A., Gray, J.: Understanding the algorithms: YouTube attempts to avoid problematic content (2019). Available from https://www.nzherald.co.nz/business/news/article.cfm?C_id=3&objectid=1228137
44. May-Chahal, C., Palmer, E.: Rapid evidence assessment characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation (2018). Available at www.iicsa.org.uk
45. McGuire, M., Dowling, S.: Cyber Crime: A Review of the Evidence. Home Office, London (2013)
46. Meredith, J.: Analysing technological affordances of online interactions using conversation analysis. J. Pragmat. **115**, 42–55 (2017)
47. Mews, A., Di Bella, L., Purver, M.: Impact evaluation of the prison-based Core Sex Offender Treatment Programme. Ministry of Justice (2017). Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623876/sotp-report-web-.pdf
48. Middleton, D., Mandeville-Norden, R., Hayes, E.: Does treatment work with Internet sex offenders? Emerging findings from the Internet sex offender treatment programme (i-SOTP). J. Sex. Aggress. **15**(1), 5–19 (2009)
49. Miraz, M., Ali, M., Excell, P., Picking, R.: Internet of nano-things, things and everything: future growth trends. Future Internet **10**(8), 68 (2018)
50. Miro-Llinares, F., Moneva, A.: What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?". Crime Sci. **8**, 12 (2019). https://doi.org/10.1186/s40163-019-0107-y
51. Mitchell, K.J., Finkelhor, D., Jones, L.M., Wolak, J.: Use of social networking sites in online sex crimes against minors: an examination of national incidence and means of utilization. J. Adolesc. Health **47**(2), 183–190 (2010)
52. Moreno, M.A., D'Angelo, J.: Social media intervention design: applying an affordances framework. J. Med. Internet Res. **21**(3), e11014 (2019). https://doi.org/10.2196/11014
53. Norman, D.A.: The Psychology of Everyday Things. Basic Books, New York (1988)
54. Pashang, S., Khanlou, N., Clarke, J.: The mental health impact of cyber sexual violence on youth identity. Int. J. Ment. Health Addict. **17**(5), 1119–1131 (2019)
55. Quayle, E.: Researching Online Child Sexual Exploitation and Abuse: Are There Links Between Online and Offline Vulnerabilities? Global Kids Online, London (2016). Available at www.globalkidsonline.net/sexual-exploitation
56. Quayle, E., Koukopoulos, N.: Deterrence of online child sexual abuse and exploitation. Policing, J. Policy Pract. **13**(3), 345–362 (2018)
57. Quayle, E., Allegro, S., Hutton, L., Sheath, M., Lööf, L.: Rapid skill acquisition and online sexual grooming of children. Comput. Hum. Behav. **39**, 368–375 (2014)
58. Reyns, B., Fisher, W., Bossler, B., Holt, S.: Opportunity and self-control: do they predict multiple forms of online victimization? Am. J. Crim. Justice **44**(1), 63–82 (2019)
59. Robey, D., Anderson, C., Raymond, B.: Information technology, materiality, and organizational change: a professional odyssey. J. Assoc. Inf. Syst. **14**(7), 386–389 (2013)

60. Sarre, R., Lau, L.Y.-C., Chang, L.Y.C.: Responding to cybercrime: current trends. Police Pract. Res. **19**(6), 515–518 (2018)
61. Seto, M.C.: The motivation-facilitation model of sexual offending. Sex. Abus. J. Res. Treat. **31**(1), 3–24 (2019)
62. Share, M., Williams, C., Kerrins, L.: Displaying and performing: Polish transnational families in Ireland Skyping grandparents in Poland. New Media Soc. **20**(8), 3011–3028 (2018)
63. Shields, M., Tonmyr, L., Hovdestad, W.: The decline of child sexual abuse in Canada: evidence from the 2014 general social survey. Can. J. Psychiatry **64**(9), 638–646 (2019)
64. Staksrud, E., Ólafsson, K., Livingstone, S.: Does the use of social networking sites increase children's risk of harm? Comput. Hum. Behav. **29**(1), 40–50 (2012)
65. Steel, C.: Web-based child pornography: the global impact of deterrence efforts and its consumption on mobile platforms. Child Abuse Neglect **44**, 150–158 (2015)
66. Steel, C., Newman, E., O'Rourke, S., Quayle, E.: An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. Forensic Sci. Int., Digit. Investig. **33**, 300971 (2020). https://doi.org/10.1016/j.fsidi.2020.300971
67. Taylor, M.: Criminogenic qualities of the Internet. Dyn. Asymmetric Confl., Comput. Assist. Terrorism **8**(2), 97–106 (2015)
68. Taylor, M., Quayle, E.: The Internet and abuse images of children: search precriminal situations and opportunity. In: Wortley, R., Smallbone, S. (eds.) Situational Prevention of Child Sexual Abuse. Crime Prevention Studies, vol. 19. Willan Publishing, Monsey (2006)
69. Taylor, M., Quayle, E.: Criminogenic qualities of the Internet in the collection and distribution of abuse images of children. In: McCarthy, J., Quayle, E., Aylwin, S., Lyddy, F. (eds.) Applying Psychology: A Festschrift for Dr Elizabeth A. Dunne. Irish Journal of Psychology, vol. 29, pp. 119–130. (2008).
70. Vaidhyanathan, S.: The Googlization of Everything (and Why We Should Worry). University of California Press, Berkeley (2011)
71. Wager, N., Armitage, R., Christmann, K., Gallagher, B., Ioannou, M., Parkinson, S., et al.: Rapid evidence assessment: quantifying the extent of online-facilitated child sexual abuse: Report for the Independent Inquiry into Child Sexual Abuse (2018). Available at http://cdn.basw.co.uk/upload/basw_103534-9.pdf
72. Wall, D.S.: Crime, security and information communication technologies: the changing cybersecurity threat landscape and implications for regulation and policing. In: Brownsword, R., Scotford, E., Yeung, K. (eds.) The Oxford Handbook on the Law and Regulation of Technology. Oxford University Press, Oxford (2017)
73. Walsh, W., Wolak, J., Finkelhor, D.: Prosecution Dilemmas and Challenges for Child Pornography Crimes: The Third National Juvenile Online Victimization Study (NJOV-3). Crimes against Children Research Center, Durham (2013)
74. Wellman, B., Quan-Haase, A., Boase, J., Chen, W., Hampton, K., Ila de Diaz, I., et al.: The social affordances of the Internet for networked individualism. J. Comput.-Mediat. Commun. **8**(3), 1–43 (2003)
75. Wolak, J., Finkelhor, D., Mitchell, K.: Trends in Arrests for Child Pornography Possession: The Third National Juvenile Online Victimization Study (NJOV-3). Crimes against Children Research Center, Durham (2012)
76. Wortley, R.: Exploring the person-situation interaction in situational crime prevention. In: Tilley, N., Farrell, G. (eds.) The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke, pp. 184–193. Routledge, London (2012)